

Sub
as

What is claimed is:

1. In a computing environment having a connection to a network, a computer program product for securely propagating security credentials using a trusted authenticating domain, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for establishing a secure connection between a client and a password synchronization agent (PSA);

computer-readable program code means for transmitting an identifier of a user and an identifying secret of the user to the PSA;

computer-readable program code means for validating the user with the trusted authenticating domain using the transmitted user identifier and identifying secret; and

computer-readable program code means for propagating the identifying secret of the user to a master registry if the validation succeeds.

2. The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a second secure connection between the PSA and the trusted authenticating domain; and

computer-readable program code means for using the second secure connection for the validating of the user.

3. The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a third secure connection

3 between the PSA and the master registry; and
4 computer-readable program code means for using the third secure connection for the
5 propagating of the identifying secret to the master registry.

1 4. The computer program product according to Claim 1, further comprising computer-
2 readable program code means for propagating the identifying secret to one or more other target
3 registries if the validation succeeds.

1 5. The computer program product according to Claim 4, further comprising:
2 computer-readable program code means for establishing additional secure connections
3 between the PSA and each of the other target registries; and
4 computer-readable program code means for using the additional secure connections for
5 the propagating of the identifying secret to the other target registries.

1 6. The computer program product according to Claim 1, further comprising:
2 computer-readable program code means for obtaining an identification of the trusted
3 authenticating domain from the user; and
4 computer-readable program code means for verifying that the trusted authenticating
5 domain is trusted by the master registry as a prerequisite to the propagating.

1 7. The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for obtaining an identification of the trusted
3 authenticating domain from the master registry.

1 8. The computer program product according to Claim 6, wherein the master registry stores
2 trust policy information, and wherein the computer-readable program code means for verifying
3 that the trusted authenticating domain is trusted further comprises computer-readable program
4 code means for checking whether the stored trust policy information for the user includes the
5 identification obtained from the user.

1 9. The computer program product according to Claim 6, wherein the master registry stores
2 trust policy information, and wherein the computer-readable program code means for verifying
3 that the trusted authenticating domain is trusted further comprises computer-readable program
4 code means for checking whether the stored trust policy information for a user group of which
5 the user is a member includes the identification obtained from the user.

1 10. The computer program product according to Claim 7, wherein the master registry stores
2 trust policy information, and wherein the computer-readable program code means for obtaining
3 the identification of the trusted authenticating domain from the master registry further comprises
4 computer-readable program code means for obtaining the identification using the stored trust
5 policy information for the user.

1 11. The computer program product according to Claim 7, wherein the master registry stores
2 trust policy information, and wherein the computer-readable program code means for obtaining
3 the identification of the trusted authenticating domain from the master registry further comprises
4 computer-readable program code means for obtaining the identification using the stored trust
5 policy information for a user group of which the user is a member.

1 12. The computer program product according to Claim 4, wherein the master registry stores
2 password synchronization policy information, and wherein the computer-readable program code
3 means for propagating the identifying secret to the one or more other target registries further
4 comprises computer-readable program code means for identifying the one or more other target
5 registries using the stored password synchronization policy information for the user.

1 13. The computer program product according to Claim 4, wherein the master registry stores
2 password synchronization policy information, and wherein the computer-readable program code
3 means for propagating the identifying secret to the one or more other target registries further
4 comprises computer-readable program code means for identifying the one or more other target
5 registries using the stored password synchronization policy information for a user group of which
6 the user is a member.

1 14. The computer program product according to Claim 1, wherein the computer-readable
2 program code means for establishing the secure connection further comprises computer-readable

3 program code means for authenticating the PSA to the client.

1 15. The computer program product according to Claim 2, wherein the computer-readable
2 program code means for establishing the second secure connection further comprises computer-
3 readable program code means for authenticating the trusted authenticating domain to the PSA.

1 16. The computer program product according to Claim 3, wherein the computer-readable
2 program code means for establishing the third secure connection further comprises computer-
3 readable program code means for authenticating the master registry to the PSA.

1 17. The computer program product according to Claim 5, wherein the computer-readable
2 program code means for establishing additional secure connections further comprises computer-
3 readable program code means for authenticating the other target registries to the PSA.

1 18. The computer program product according to Claim 1, wherein the computer-readable
2 program code means for validating further comprises:

3 computer-readable program code means for performing a security function on the
4 identifying secret of the user, wherein the security function comprises one of (i) a one-way
5 hashing algorithm or (ii) an encryption algorithm;

6 computer-readable program code means for using the user identifier to locate a
7 previously-stored identifying secret of the user which was stored by the trusted authenticating

8 domain; and

9 computer-readable program code means for comparing the located identifying secret to a
10 result of performing the security function.

1 19. The computer program product according to Claim 1, wherein the computer-readable
2 program code means for validating further comprises computer-readable program code means for
3 invoking an authenticated LDAP bind or other native authentication mechanism of the trusted
4 authenticating domain, wherein the identifier of the user and the identifying secret of the user are
5 passed to the trusted authenticating domain, thereby causing the trusted authenticating domain to
6 validate the passed identifier and identifying secret and return a result which reports a success or
7 failure of the validation.

1 20. The computer program product according to Claim 1, wherein the PSA has administrative
2 authority for performing operations at the master registry.

1 21. The computer program product according to Claim 4, wherein the PSA has administrative
2 authority for performing operations at the one or more other target registries.

1 22. A system for securely propagating security credentials using a trusted authenticating
2 domain, comprising:

3 means for establishing a secure connection between a client and a password

4 synchronization agent (PSA);

5 means for transmitting an identifier of a user and an identifying secret of the user to the
6 PSA;

7 means for validating the user with the trusted authenticating domain using the transmitted
8 user identifier and identifying secret; and

9 means for propagating the identifying secret of the user to a master registry if the
10 validation succeeds.

1 23. The system according to Claim 22, further comprising:

2 means for establishing a second secure connection between the PSA and the trusted
3 authenticating domain; and

4 means for using the second secure connection for the validating of the user.

1 24. The system according to Claim 22, further comprising:

2 means for establishing a third secure connection between the PSA and the master registry;
3 and

4 means for using the third secure connection for the propagating of the identifying secret
5 to the master registry.

1 25. The system according to Claim 22, further comprising means for propagating the
2 identifying secret to one or more other target registries if the validation succeeds.

1 26. The system according to Claim 25, further comprising:
2 means for establishing additional secure connections between the PSA and each of the
3 other target registries; and
4 means for using the additional secure connections for the propagating of the identifying
5 secret to the other target registries.

1 27. The system according to Claim 22, further comprising:
2 means for obtaining an identification of the trusted authenticating domain from the user;
3 and
4 means for verifying that the trusted authenticating domain is trusted by the master registry
5 as a prerequisite to the propagating.

1 28. The system according to Claim 22, further comprising:
2 means for obtaining an identification of the trusted authenticating domain from the master
3 registry.

1 29. The system according to Claim 27, wherein the master registry stores trust policy
2 information, and wherein the means for verifying that the trusted authenticating domain is trusted
3 further comprises means for checking whether the stored trust policy information for the user
4 includes the identification obtained from the user.

1 30. The system according to Claim 27, wherein the master registry stores trust policy
2 information, and wherein the means for verifying that the trusted authenticating domain is trusted
3 further comprises means for checking whether the stored trust policy information for a user group
4 of which the user is a member includes the identification obtained from the user.

1 31. The system according to Claim 28, wherein the master registry stores trust policy
2 information, and wherein the means for obtaining the identification of the trusted authenticating
3 domain from the master registry further comprises means for obtaining the identification using
4 the stored trust policy information for the user.

1 32. The system according to Claim 28, wherein the master registry stores trust policy
2 information, and wherein the means for obtaining the identification of the trusted authenticating
3 domain from the master registry further comprises means for obtaining the identification using
4 the stored trust policy information for a user group of which the user is a member.

1 33. The system according to Claim 25, wherein the master registry stores password
2 synchronization policy information, and wherein the means for propagating the identifying secret
3 to the one or more other target registries further comprises means for identifying the one or more
4 other target registries using the stored password synchronization policy information for the user.

1 34. The system according to Claim 25, wherein the master registry stores password
2 synchronization policy information, and wherein the means for propagating the identifying secret
3 to the one or more other target registries further comprises means for identifying the one or more
4 other target registries using the stored password synchronization policy information for a user
5 group of which the user is a member.

1 35. The system according to Claim 22, wherein the means for establishing the secure
2 connection further comprises means for authenticating the PSA to the client.

1 36. The system according to Claim 23, wherein the means for establishing the second secure
2 connection further comprises means for authenticating the trusted authenticating domain to the
3 PSA.

1 37. The system according to Claim 24, wherein the means for establishing the third secure
2 connection further comprises means for authenticating the master registry to the PSA.

1 38. The system according to Claim 26, wherein the means for establishing additional secure
2 connections further comprises means for authenticating the other target registries to the PSA.

1 39. The system according to Claim 22, wherein the means for validating further comprises:
2 means for performing a security function on the identifying secret of the user, wherein the

3 security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption
4 algorithm;

5 means for using the user identifier to locate a previously-stored identifying secret of the
6 user which was stored by the trusted authenticating domain; and

7 means for comparing the located identifying secret to a result of performing the security
8 function.

1 40. The system according to Claim 22, wherein the means for validating further comprises
2 means for invoking an authenticated LDAP bind or other native authentication mechanism of the
3 trusted authenticating domain, wherein the identifier of the user and the identifying secret of the
4 user are passed to the trusted authenticating domain, thereby causing the trusted authenticating
5 domain to validate the passed identifier and identifying secret and return a result which reports a
6 success or failure of the validation.

1 41. The system according to Claim 22, wherein the PSA has administrative authority for
2 performing operations at the master registry.

1 42. The system according to Claim 25, wherein the PSA has administrative authority for
2 performing operations at the one or more other target registries.

